Sous-groupes distingués, groupes quotients.

Par Nicolas Lanchier [1]

1 Propriétés classiques. Théorèmes d'isomorphismes.

Définition 1.1 — Soient G un groupe et H un sous-groupe G. On dit que H est distingué dans G, ce que l'on note $H \lhd G$, si H est invariant par automorphismes intérieurs, i.e.

$$\forall\ x \in G \qquad x \cdot H = H \cdot x$$

[4], Sect. 1.2

Proposition 1.2 — $H \lhd G$ si et seulement si pour tout $x \in G$, $x \cdot H \cdot x^{-1} \subset H$.

Théorème 1.3 — H est distingué dans G si et seulement s'il existe un groupe K et un homomorphisme $\varphi : G \longrightarrow K$ tels que $H = \operatorname{Ker} \varphi$.

Théorème 1.4 — Une relation d'équivalence $\sim$ sur G est compatible avec la structure de groupe de G si et seulement s'il existe $H \lhd G$ tel que pour tous $x, y \in G$, $x \sim y \iff x \cdot y^{-1} \in H$. Dans ce cas, le quotient $G/\sim$, également noté G/H, est naturellement muni d'une structure de groupe.

Définition 1.5 — Le groupe G/H est appelé groupe quotient de G par H.

Théorème 1.6 — Soient G, K deux groupes, H un sous-groupe distingué de G, $\varphi : G \longrightarrow K$ un homomorphisme et π la projection canonique de G sur G/H. Supposons que $H \subset \operatorname{Ker} \varphi$. Alors il existe un unique homomorphisme $\psi : G/H \longrightarrow K$ tel que $\psi \circ \pi = \varphi$.

Théorème 1.7 (premier théorème d'isomorphisme) — Soit $\varphi : G \longrightarrow H$ un morphisme de groupe. Alors $\operatorname{Im} \varphi \cong G/\operatorname{Ker} \varphi$. [1], Sect. 4.4

Théorème 1.8 (second théorème d'isomorphisme) — Soient G un groupe et $H \lhd G$. Alors pour tout sous-groupe K de G

$$H \cap K \lhd K \qquad H \lhd H \cdot K \qquad \text{et} \qquad \frac{K}{H \cap K} \cong \frac{H \cdot K}{H}$$

[1], Sect. 4.4

Théorème 1.9 (troisième théorème d'isomorphisme) — Soient G un groupe, H et K deux sous-groupes distingués de G avec $H \subset K$. Alors

$$K/H \lhd G/H \qquad \text{et} \qquad G/K \cong \frac{G/H}{K/H}$$

[1], Sect. 4.4

2 Groupe de Galois et points constructibles.

Définition 2.1 — Le groupe de Galois d'une extension de corps $K \subset L$ est le groupe, noté $\operatorname{Gal}(L|K)$, des K-automorphismes de L, i.e. des automorphismes $\sigma : L \longrightarrow L$ tels que pour tout $x \in K$, $\sigma(x) = x$. [2], Sect. 8.5

Définition 2.2 — Le groupe de Galois d'un polynôme $P \in K[X]$ est, par définition, le groupe $\operatorname{Gal}(L|K)$ où L est le corps de décomposition de P sur K. [2], Sect. 8.5

Théorème 2.3 (correspondance de Galois) — Soient $K \subset N$ et $K \subset L$ deux extensions normales avec $L \subset N$. Alors

1. $\operatorname{card} \operatorname{Gal}(N|K) = [N : K]$;
2. il existe une bijection $H \mapsto \operatorname{inv}(H)$ de l'ensemble des sous-groupes de G sur l'ensemble des corps intermédiaires entre K et N ;
3. $\operatorname{Gal}(N|L)$ est un sous-groupe distingué de $\operatorname{Gal}(N|K)$;
4. le groupe quotient $\operatorname{Gal}(N|K)/\operatorname{Gal}(N|L)$ est isomorphe à $\operatorname{Gal}(L|K)$.

Théorème 2.4 — Un p-groupe G possède des sous-groupes distingués à tous les ordres divisant l'ordre de G. [3], Sect. 1.4

Application 2.5 — Soient L un sous-corps de $\mathbb{R}$ et $(x, y) \in L^2$. Si l'extension $\mathbb{Q} \subset L$ est normale de degré une puissance de 2 alors le point (x, y) est constructible à la règle et au compas. [3], Ex 4.14

3 Groupes résolubles et résolubilité des équations par radicaux.

Définition 3.1 — Un groupe fini G est dit résoluble s'il existe une suite finie G_0, $G_1 \dots G_r$ de sous-groupes de G, appelée suite de résolubilité, telle que

1. $\{e\} = G_r \subset G_{r-1} \subset \cdots \subset G_0 = G$;
2. G_{i+1} est distingué dans G_i pour tout $0 \leq i \leq r-1$;
3. G_i/G_{i+1} est un groupe commutatif pour tout $0 \leq i \leq r-1$.

De façon équivalente, un groupe G est résoluble s'il existe un entier s tel que $D^s(G) = \{e\}$, où $D(G)$ désigne le groupe engendré par les commutateurs de G. [2], Ch. 11

Définition 3.2 — Une extension $K \subset L$ est dite radicale s'il existe une tour de corps K_1, $K_2 \dots K_r$, appelée tour radicale, telle que

1. $K = K_0 \subset K_1 \subset \cdots \subset K_r = L$;
2. Pour tout $1 \leq i \leq r$, il existe $a_i \in K_i$ et $n_i \geq 1$ tels que $K_i = K_{i-1}[a_i]$ et ${a_i}^{n_i} \in K_{i-1}$.

[2], Ch. 12

Théorème 3.3 (Galois) — Si un polynôme P est résoluble par radicaux alors son groupe de Galois est résoluble. [2], Ch. 12

Théorème 3.4 — Le polynôme $P(X) = X^5 - 10X + 5$ de $\mathbb{Q}[X]$ n'est pas résoluble par radicaux. [2], Sect. 12.3

Références

[1] Josette Calais. *Eléments de théorie des groupes.* Puf, 1998.

[2] Jean-Pierre Escofier. *Théorie de Galois, cours et exercices corrigés.* Dunod, 1997.

[3] Hervé Francinou, Serge Gianella. *Exercices de mathématiques pour l'agrégation, algèbre 1.* Masson, 1995.

[4] Daniel Perrin. *Cours d'algèbre.* Ellipses, 1996.